

Nortel Networks

Contivity Stateful Firewall

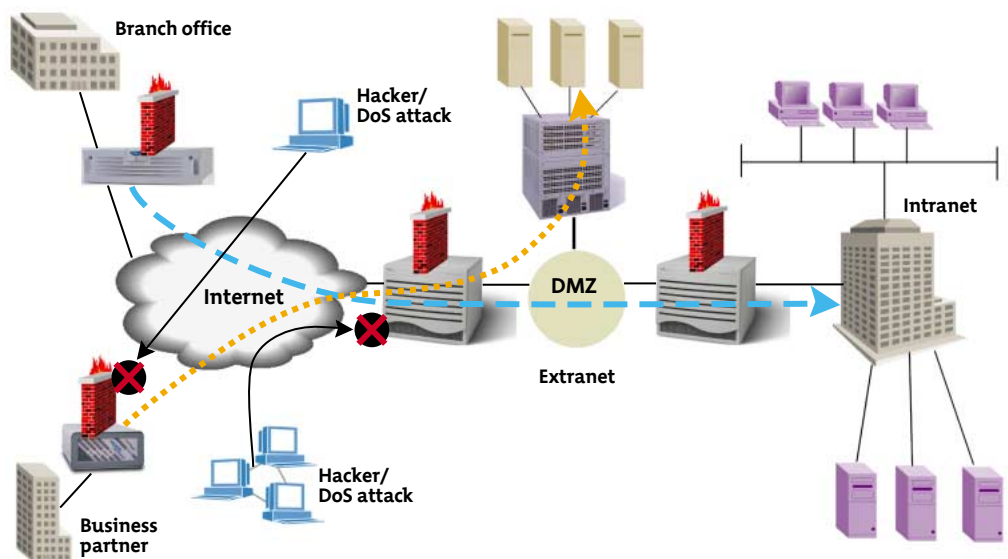
This powerful, high-performance stateful firewall, tightly integrated with our industry-leading Contivity IP VPN family, creates a complete security solution. One GUI to manage all features (firewall, VPN, routing) means substantial savings compared to other products. One device for firewall, VPN, and routing reduces your hardware and support personnel expenses.

Firewall protection

The Contivity VPN Switch combines a stateful firewall, network address translation (NAT), and sophisticated packet filters to provide security to your network and protection of your data from unauthorized external intrusion. The firewall provides a line of defense to allow acceptable traffic—as defined by your security policy—to pass through while dropping all other traffic before it enters or leaves the network. It monitors packets and sessions to make decisions based on established rules to determine the appropriate actions to take.

Stateful inspection

By using stateful inspection, the Contivity Stateful Firewall provides a very high level of security and performance, with superior flexibility to define the rules to fit your environment.



The Contivity Stateful Firewall delivers full firewall capabilities by examining both incoming and outgoing packets running against a common security policy. All service rules are interpreted on IP conversations, or the “packet state,” significantly improving performance.

**NORTEL
NETWORKS™**

Complex protocols—FTP, TELNET, H.323, RealAudio, etc.—require special handling. The Contivity Stateful Firewall can handle these, and over 100 IP protocols, achieving peak performance through advanced memory management techniques and optimized packet inspection.

Flexible logging and filtering

The Contivity Stateful Firewall can classify packets on any of the multiple interfaces—physical or virtual (tunnels, end user or branch)—available on the Contivity VPN Switch, capturing both public and private traffic.

Conversely, rules in your policy can be set to “Any,” therefore applying to all interfaces, or all protocols.

Security policies on the Contivity Stateful Firewall are built off the following parameters:

- Source interface (tunnel, physical or any)
- Destination interface
- Source address (mask), Destination address (mask)
- Service (protocol, source port, or destination port)
- Action (accept, drop, or reject)
- Log (log and/or trap)
- State (enabled or disabled)
- Remark (used for a comment)

In addition, you can configure the firewall to log some or all significant events. This includes all connections over the network, such as email transactions, firewall status changes, and system failures. This preserves a detail-rich audit trail for troubleshooting any network problems.

Contivity Stateful Firewall advanced features include:

- Anti-spoofing
- Denial of Service (DoS) attacks
 - Ping of death
 - Syn Flood
 - UDP bomb
 - Land attack
 - Smurf
 - Fraggle
 - ICMP unreachable
- DoS bins—protection of system resources
 - SYN and FIN bin
 - Half-conversation bin

Superior performance

The Contivity Stateful Firewall can support up to 500,000 concurrent sessions, adding over 20,000 sessions per second. Additionally, the Firewall can statefully inspect over 400 Mbps of data. VPN encryption rates exceed line rates, providing over 140 Mbps of 3DES encryption.

Benefits

- Standalone CPE device that supports VPN, IP routing, proxy and Stateful Firewall capabilities, NAT, and protection against DoS attacks
- Based on high-performance ICSA-certified stateful inspection engine
- Extensive filtering and logging of tunneled and non-tunneled traffic from any interface (public or private) and/or any VPN tunnel
- Management of the Contivity's VPN, routing, or firewall functionality via a simple network browser, eliminating the need for expensive firewall management consoles

Requirements

For each Contivity VPN switch on which you want to install the Contivity Stateful Firewall, you will need:

- Server software version 3.5 or later
- A license key per switch on which you want the firewall



For more information, contact your Nortel Networks representative, or call 1-800-4 NORTEL or 1-800-466-7835 from anywhere in North America.

<http://www.nortelnetworks.com>

*Nortel Networks, the Nortel Networks logo, and Contivity are trademarks of Nortel Networks. All other trademarks are the property of their owners

Copyright © 2001 Nortel Networks. All rights reserved. Information in this document is subject to change without notice. Nortel Networks assumes no responsibility for any errors that may appear in this document.